First Point srl
Via Milano 50DX – 43036 Fidenza (PR)
Tel: +39.0524.533301 – Fax: +39.0524.510224
info@firstpoint.it – PEC firstpoint@pec.firstpoint.it
www.firstpoint.it
P.IVA e C.F.: 02375140346

INFORMATIVA SULLA SICUREZZA DEI SERVIZI CLOUD

Articolo 1 - Ambito di applicazione,

1.1 La presene informativa trova applicazione solo nel caso in cui il Cliente abbia sottoscritto un Modulo d'Ordine per la fornitura dei Servizi Cloud in conformità a quanto previsto all'articolo 1 delle Condizioni Generali di Contratto e vanno ad ampliare le indicazioni inserite nel documento "Condizioni specifiche dei servizi Cloud".

Articolo 2 – Responsabilità di First Point

2.1 Fermi restando gli obblighi a proprio carico già previsti nelle Condizioni Generali di Contratto e nelle Condizioni specifiche dei servizi Cloud First Point si impegna ad effettuare le seguenti attività:

•Gestione e manutenzione dell'infrastruttura per mantenerla efficiente ed aggiornata.

• Limitare l'accesso al servizio Cloud del cliente solo agli utenti da lui autorizzati.

•Configurare i sistemi cloud in modo sicuro per i servizi cloud.

•Informare i clienti di modifiche che possono impattare la sicurezza.

•Monitorare la sicurezza dell'infrastruttura.

•Implementare le misure di sicurezza hardware e software.

•Ove previsto dal servizio, eseguire i backup regolarmente.

•Applicare tutti gli aggiornamenti necessari al fine di mantenere l'ambiente Cloud aggiornato e sicuro.

•Gestire e monitorare gli strumenti di crittografia.

•Gestire eventuali incidenti per garantire che non vengano diffusi dati sensibili e che non influiscano sulla sicurezza e sulla qualità del servizio.

•Fornire informazioni su servizio, backup e sicurezza su richiesta

•Informare i clienti su vulnerabilità e mitigazioni secondo le indicazioni fornite nel medesimo documento.

Articolo 3 - Responsabilità del Cliente

3.1 Fermi restando tutti gli obblighi a proprio carico previsti nelle Condizioni Generali di Contratto e nelle Condizioni specifiche dei servizi Cloud, con espresso riferimento ai Servizi Cloud il Cliente si impegna a:

•Gestire le credenziali di accesso.

•Monitorare l'utilizzo delle risorse cloud.

•Verificare che i controlli di sicurezza forniti siano adeguati.

•Richiedere l'installazione di patch specifiche.

•Segnalare eventuali incidenti.

Articolo 4 – Diritto di controllo

4.1 Il cliente ha il diritto di richiedere, con un congruo preavviso, report periodici sulle misure di sicurezza.

4.2 First Point effettua verifiche interne delle proprie misure di sicurezza, al fine di:

- Assicurarsi della corretta implementazione e manutenzione dei controlli di sicurezza
- Identificare eventuali vulnerabilità
- Implementare le correzioni necessarie

Tali verifiche interne vengono effettuate indipendentemente dalle richieste dei clienti e hanno lo scopo di migliorare continuamente il livello di sicurezza dei servizi forniti.

Articolo 5 - Comunicazione dei dati

5.1 Le richieste di comunicazione dei dati da parte di terzi dovranno provenire solo dal cliente o dai suoi referenti autorizzati, indicati nell'accordo. Tutte le altre richieste saranno respinte.

5.2 In caso di richieste da parte delle forze dell'ordine, First Point seguirà una procedura specifica, informando contestualmente il cliente. Per le altre richieste, First Point informerà il cliente e attenderà istruzioni.

Articolo 6 – Crittografia dei dati

6.1 Non viene mai concesso l'accesso diretto ai server senza adeguate misure di sicurezza. Per connettersi ai server è necessario utilizzare canali VPN cifrati. I servizi vengono forniti su protocolli cifrati come Https e con autorizzazione via IP.

Vengono applicati protocolli crittografici sia per gli accessi sia per l'immissione dei dati

Articolo 7 – Uso di subfornitori

7.1 Il cliente acconsente all'uso di subfornitori da parte di First Point per l'esecuzione di operazioni di trattamento dati, a meno che non specifichi diversamente.

I subfornitori non situati nello Spazio Economico Europeo adottano almeno una delle seguenti misure:

- Dichiarazione di adeguatezza del paese da parte della Commissione Europea
- Binding Corporate Rules confermate dalla Commissione Europea.
- Contratto con clausole contrattuali per la protezione dei dati, qualora ne avessero accesso.

7.2 L'uso di subfornitori critici per la sicurezza dei servizi Cloud è condizionato alla stipula di un contratto che

First Point srl
Via Milano 50DX – 43036 Fidenza (PR)
Tel: +39.0524.533301 – Fax: +39.0524.510224
info@firstpoint.it – PEC firstpoint@pec.firstpoint.it
www.firstpoint.it
P.IVA e C.F.: 02375140346

includa gli stessi (o più stringenti) requisiti di quello con First Point.

Articolo 8 - Gestione utenze e autorizzazioni ai servizi

8.1 Per i servizi di trasmissione dati e telefonia (CVT): Sono fornite utenze standard ai clienti. Queste permettono l'accesso ai servizi di base come l'invio e ricezione di chiamate, dati e messaggi. Questo tipo di utenza è la più basilare e generalmente non ha accesso limitato alle funzionalità avanzate.

8.2 Per i servizi di hosting: sono fornite utenze di amministrazione. Queste permettono ai clienti di installare e gestire i propri siti web, database ed altre risorse ospitate sui server del provider. Solitamente le utenze di amministrazione danno accesso pieno alla configurazione e gestione delle risorse assegnate.

8.3 Per i servizi di backup on line: anche in questo caso le utenze fornite sono di tipo amministratore, in modo da permettere ai clienti di configurare e gestire in autonomia i propri piani di backup e ripristino dati archiviati sul cloud.

Queste utenze sono attivate di default, si possono personalizzare i tipi di utenza in base alle richieste del cliente in maniera differente per ogni singolo servizio

Articolo 9 – Monitoraggio dei log

9.1 Il provider First Point dispone di avanzati strumenti di monitoraggio per tutti i servizi erogati.

Quando si verificano determinate condizioni critiche, come, a titolo di esempio:

• Troppi tentativi di accesso non autorizzato
• Superamento dei limiti contrattuali delle risorse
• Rilevamento dal firewall

Il cliente viene allertato tempestivamente qualora dal monitoraggio dei log si rilevassero dei problemi di sicurezza rilevanti che comprometterebbero il servizio e portassero ad una perdita di dati

9.2 I log, vengono raccolti e archiviati tramite strumenti di log collecting che consentono anche di proteggerli grazie ai controlli di sicurezza implementati

Articolo 10 – Gestione degli incidenti

10.1 Sono considerati incidenti di sicurezza gli eventi che mettono a rischio la riservatezza, integrità e disponibilità delle informazioni.

Tra gli esempi principali di incidenti:

• Guasti e furti di dispositivi
• Errori umani
• Violazioni di norme di sicurezza fisica e logica
• Accessi non autorizzati ai sistemi
• Indisponibilità dei sistemi informatici

10.2 Tutti gli eventi, incidenti e vulnerabilità devono essere tempestivamente comunicati al reparto IT tramite l'help desk aziendale, per avviare le procedure opportune.

10.3 Nel caso di interruzioni prolungate o alterazioni illegittime di dati, il Direttore Commerciale informa il cliente. Vengono effettuate analisi approfondite per determinare quali dati (soprattutto personali) sono stati compromessi.

10.4 In caso di incidenti viene redatta una relazione contenente:

• Descrizione dell'evento
• Data e orario di occorrenza e segnalazione
• Azioni intraprese
• Elementi che hanno reso l'incidente risolto
• Data di chiusura

Articolo 11 – Gestione incidenti con impatto su dati personali

11.1 In caso di incidenti che coinvolgono dati personali, il Responsabile della Sicurezza Informazione (RGSI) ne informa la Direzione. La Direzione valuta se la violazione dei dati comporta un rischio per i diritti e le libertà delle persone fisiche.

11.2 Se il rischio sussiste, la Direzione segnala:

- entro 72 ore al Garante per la protezione dei dati personali (qualora First Point fosse titolare del trattamento);
- entro 24 ore agli enti titolari dei dati coinvolti.

La notifica al Garante riporta:

a) la descrizione dell'incidente
b) quantità e categorie di dati interessati
c) i dati del responsabile del trattamento (First Point)
d) le probabili conseguenze
e) le misure per rimediare e attenuare gli effetti dell'incidente

11.3 La stessa notifica viene inviata agli interessati, salvo che:

- i dati siano crittografati/incomprensibili
- siano state adottate misure che limitano l'impatto sugli interessati

La Direzione è tenuta ad informare tempestivamente i soggetti coinvolti in caso di violazioni reali o potenziali di dati personali, al fine di tutelare la privacy e la sicurezza delle informazioni.

11.4 Il riferimento per il trattamento dei dati personali è:

First Point srl
Via Milano 50DX – 43036 Fidenza (PR)
Tel: +39.0524.533301 – Fax: +39.0524.510224
info@firstpoint.it – PEC firstpoint@pec.firstpoint.it
www.firstpoint.it
P.IVA e C.F.: 02375140346

Titolare del Trattamento dei Dati
First Point Srl
via Milano 50dx
43036 Fidenza (PR)
Email: info@firstpoint.it

12. Raccolta di prove

12.1 In caso di necessità, la Direzione può decidere di raccogliere prove degli incidenti di sicurezza, anche per poter identificare e perseguire i responsabili o su richiesta delle autorità. I clienti possono richiedere l'acquisizione di prove, ma prima di procedere devono contattare la Direzione con richiesta formale via pec.

12.2 I tecnici First Point devono collaborare per non compromettere i servizi attivi (nel caso di acquisizioni dati in tempo reale) e garantire la raccolta delle prove, la Direzione valuta:

- L'opportunità e le implicazioni legali
- Il modo migliore per acquisire le prove minimizzando il rischio di danni
- Le precauzioni per proteggere i dati riservati

Le prove possono essere utili per:

- Valutare eventuali responsabilità
- Documentare l'incidente per le autorità
- Migliorare i processi di sicurezza per evitare il ripetersi

13 – Componenti fisiche e caratteristiche tecniche

13.1 Datacenter primario: Il nostro datacenter principale si trova presso la nostra sede di First Point. E' stato progettato secondo i più elevati standard di sicurezza, affidabilità e performance. L'accesso al datacenter è rigorosamente controllato 24 ore al giorno, 7 giorni alla settimana. Solo il personale autorizzato ha accesso fisico alle sale macchine. L'ambiente del datacenter è costantemente monitorato e mantenuto nelle condizioni ottimali grazie ai sistemi di condizionamento dell'aria e ridondanza elettrica degli UPS e dei gruppi elettrogeni. Tutte le apparecchiature all'interno del datacenter, tra cui server, switch e storage, sono protetti con firewall, antivirus, crittografia e altre misure di sicurezza logicali per garantire la riservatezza, integrità e disponibilità dei dati. Sono implementate misure di sicurezza fisica e logica, tra cui firewall, antivirus, rilevatori di intrusione, crittografia, per prevenire accessi non autorizzati alle risorse ospitate nel datacenter. Tutte le procedure operative e misure di sicurezza implementate nel datacenter sono conformi agli standard ISO/IEC 27001, ISO/IEC 27017 e ISO/IEC 27018 sulle migliori pratiche per la gestione della sicurezza delle informazioni.

13.2 Datacenter secondario Abbiamo anche un datacenter secondario ubicato in un'altra posizione in Italia con le medesime caratteristiche e livelli di sicurezza e affidabilità del datacenter primario. Il datacenter secondario è utilizzato per Disaster Recovery.

13.3 L'orario è ottenuto tramite NTP con la sincronizzazione con server valutati affidabili